IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

ALEXANDER FURMAN, individually and on behalf of all others similarly situated, Plaintiff, v. JP MORGAN CHASE & CO.; JPMORGAN CHASE BANK N.A.; CHASE BANK USA, N.A.; and J.P. MORGAN SECURITIES LLC; Defendants.	Case No. **JURY TRIAL DEMANDED** **CLASS ACTION COMPLAINT**

Plaintiff Alexander Furman ("Plaintiff"), individually and on behalf of all others similarly situated, complains of the actions of defendants JP Morgan Chase & Co.; JPMorgan Chase Bank N.A.; Chase Bank USA, N.A.; and J.P. Morgan Securities LLC (collectively, "Defendants"), based on his personal knowledge regarding his personal circumstances and based on information and belief and the investigation of counsel as to all other allegations, as follows:

I. NATURE OF THE CASE

1. Plaintiff and the Class Members are Defendants' banking, credit card, and investment customers, who entrusted their personally identifiable information ("PII") to Defendants. Defendants betrayed the trust of Plaintiffs and the Class by failing to properly safeguard and protect their PII and, on information and belief, publicly disclosing their Social Security Numbers without authorization in violation of numerous federal and state laws, including, *inter alia*, the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.* ("the FCRA"), and applicable common law.

2. On or about September 1, 2013, Defendants mailed a Privacy Notification to Plaintiff and the Class via the United States mail, purporting to inform their customers how

Defendants protect their PII. On the outside of the Privacy Notification sent to Plaintiff, Defendants printed his Social Security Number, together with his name and address; on information and belief, Defendants printed the respective Social Security Numbers of each respective customer, together with their name and address, on the outside of each respective Privacy Notification ("First Data Breach"). Plaintiff complained immediately and directly to Defendants about the First Data Breach.

3. Despite being on notice of the First Data Breach, on or about September 15, 2013, Defendants mailed a Benefits Notification to Plaintiffs and the Class. On the outside of the Benefits Notification sent to Plaintiff, Defendants again printed his Social Security Number, together with his name and address; on information and belief, Defendants printed the respective Social Security Numbers of each respective customer, together with their name and address, on the outside of each respective Benefits Notification ("Second Data Breach").[1]

4. Defendants flagrantly disregarded Plaintiff's and the Class Members' privacy and property rights by intentionally, willfully and recklessly failing to take the necessary precautions required to safeguard and protect Plaintiff's and the Class Members' PII from unauthorized disclosure. Plaintiff's and the Class Members' PII was improperly handled, inadequately protected, and not kept in accordance with basic security protocols. Defendants' Data Breaches represent a flagrant disregard of Plaintiff's and the Class Members' rights, both as to privacy and property.

5. As a direct and proximate result of Defendants' Data Breaches, Plaintiff and the Class Members are at an imminent, immediate and continuing increased risk of identity theft and identity fraud. Accordingly, Plaintiff and the Class Members seek redress against Defendants for,

[1] The First Data Breach and Second Data Breach, when referred to collectively, will be referred to as the "Data Breaches."

inter alia, violations of the Fair Credit Reporting Act, state consumer fraud acts, and common law. Plaintiff, on behalf of himself and the Class, seeks actual damages, statutory damages under the Fair Credit Reporting Action, and/or nominal damages, injunctive relief, and attorneys' fees and costs.

II. JURISDICTION AND VENUE

6. The Court has subject matter jurisdiction over this lawsuit, pursuant to 28 U.S.C. § 1331, because Plaintiff raises a federal question under the Fair Credit Reporting Act. This Court also has subject matter jurisdiction over this class action pursuant to 28 U.S.C. § 1332 as amended by the Class Action Fairness Act of 2005 because, on information and belief, the matter in controversy exceeds $5,000,000, exclusive of interest and costs, and is a class action in which some members of the Classes are citizens of states different than Defendant. See 28 U.S.C. § 1332(d)(2)(A).

7. This Court also has personal jurisdiction over Defendants because they are authorized to do business and in fact do business in this state and Defendants have sufficient minimum contacts with this state, and/or otherwise intentionally avail themselves of the markets in this state through the promotion, marketing and sale of their products and services in this state, to render the exercise of jurisdiction by this Court permissible under traditional notions of fair play and substantial justice.

8. Pursuant to 28 U.S.C. § 1391, venue is proper in the Northern District of Illinois because Defendants reside in this District, Defendants are found in this District, and/or Defendants are subject to personal jurisdiction in this District.

III. PARTIES

9. JP Morgan Chase & Co. ("JP Morgan") is incorporated in the state of Delaware with its principal place of business located in New York, New York. JP Morgan bills itself on its website as "a leading global financial services firm with assets of $2 trillion and operations in more than 60 countries. The firm is a leader in investment banking, financial services for consumers, small business and commercial banking, financial transaction processing, asset management, and private equity." JP Morgan and certain of its subsidiaries sent the Privacy Notification and Benefits Notification to Plaintiff and members of the class. Because the Social Security Numbers of Plaintiff and, on information and belief, the Class Members were printed on the outside of the envelopes of the Privacy Notification and Benefits Notification in violation of law, Plaintiff and the Class Members were damaged.

10. JPMorgan Chase Bank N.A. maintains its principal place of business in Columbus, Ohio. JPMorgan Chase Bank N.A. is a principal subsidiary of JP Morgan. Together with JP Morgan and certain of its subsidiaries, JPMorgan Chase Bank N.A. sent the Privacy Notification and Benefits Notification to Plaintiff and members of the class.

11. Chase Bank USA, N.A. is incorporated in the state of Delaware with its principal place of business located in Wilmington, Delaware. Chase Bank USA, N.A. is a principal subsidiary of JP Morgan. Together with JP Morgan and certain of its subsidiaries, Chase Bank USA, N.A. sent the Privacy Notification and Benefits Notification to Plaintiff and members of the class.

12. J.P. Morgan Securities LLC is incorporated in the state of Delaware with its principal place of business located in New York, New York. J.P. Morgan Securities LLC is a principal subsidiary of JP Morgan. Together with JP Morgan and certain of its subsidiaries, J.P.

Morgan Securities LLC sent the Privacy Notification and Benefits Notification to Plaintiff and members of the class.

IV. BACKGROUND FACTS

A. Identity Theft

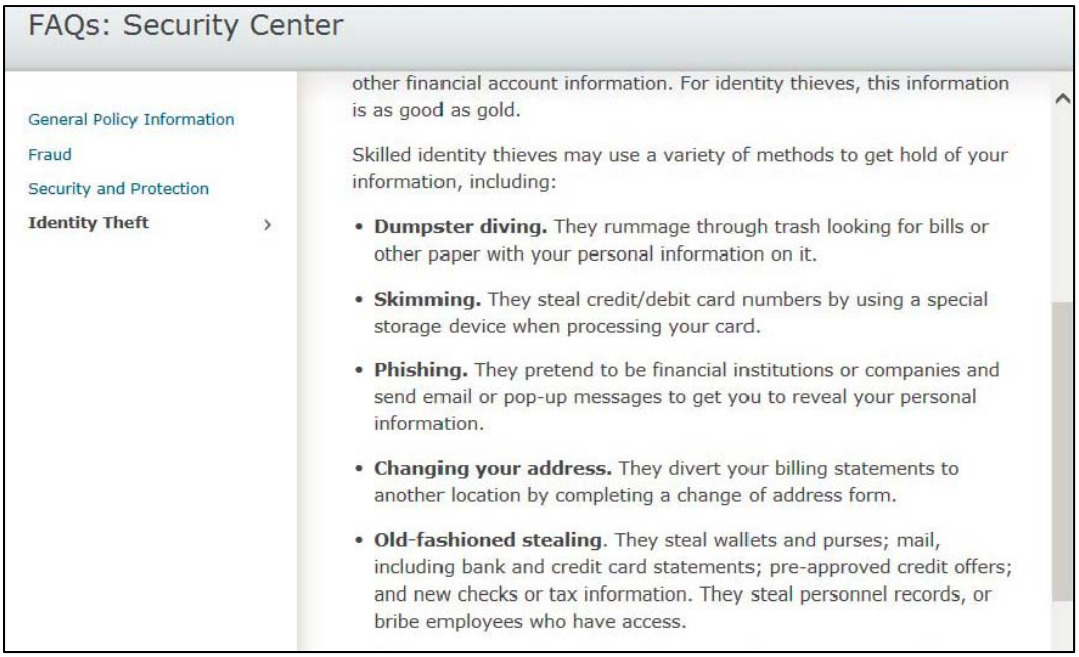
13. Identity theft occurs when someone uses an individual's PII, such as the person's name, Social Security Number, or credit card number, without the individual's permission, to commit fraud or other crimes.[2] The Federal Trade Commission explains that "[i]dentity theft is a serious crime. It can disrupt your finances, credit history, and reputation, and take time, money, and patience to resolve."

14. Similarly, Defendants admit that "[i]dentity theft happens when a criminal obtains your personal information to steal money from your accounts, open new credit cards, apply for loans, rent apartments and commit other crimes — all using your identity. These acts can damage your credit, leave you with unwanted bills and cause you countless hours and frustration to clear your good name."[3]

15. In fact, Defendants admit that a name combined with a Social Security Number is "**as good as gold**" to an identity thief. Defendants explain how thieves steal an identity:[4]

[2] *See* http://www.consumer.ftc.gov/articles/pdf-0014-identity-theft.pdf (last accessed September 16, 2013).
[3] *See* https://www.chase.com/index.jsp?pg_name=ccpmapp/privacy_security/identity_theft/page/identity_theft (last accessed September 16, 2013).
[4] *See* https://www.chase.com/resources/privacy-security (last accessed September 16, 2013).

16. Defendants also admit that identity thieves target mail for "old fashioned" stealing of PII:[5]



17. Identity theft crimes often involve more than just crimes of financial loss. Identity thieves may use stolen Social Security numbers and names to obtain a driver's license or official identification card in the victim's name but with their picture, to obtain government benefits or file a fraudulent tax return. Identity thieves also use stolen Social Security numbers to rent houses and apartments and/or obtain medical services in a victim's name. Identity thieves also

[5] https://www.chase.com/resources/privacy-security (last accessed September 16, 2013).

have been known to give a victim's PII to police during an arrest, resulting in the issuance of an arrest warrant in the victim's name and an unwarranted criminal record.

18. According to the FTC, "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[6]

19. In its 2012 Identity Fraud Report ("the Report"), Javelin Strategy & Research ("Javelin"), a leading provider of quantitative and qualitative research, quantified the impact of data breaches. According to the Report, individuals whose PII is subject to a reported data breach, like Defendants' Data Breaches, are nearly 10 times more likely than the general public to suffer identity fraud and/or identity theft. Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported, and a high probability that criminals who may now possess Plaintiff's and the Class Members' PII and not yet used the information will do so at a later date or re-sell it.

20. According to the Javelin Report, not only is there a substantially increased risk of identity theft and identity fraud for data breach victims, those who are further victimized by identity theft or identity fraud will incur an average fraud-related economic loss of $1,513 and incur an average of $354 of out-of-pocket expenses attempting to rectify the situation. Moreover, the mean resolution time of identity fraud was 12 hours of individual follow-up time.

21. The unauthorized disclosure of a person's Social Security number can be particularly damaging since Social Security numbers cannot be easily replaced like a credit card or debit card. In order to obtain a new Social Security number, a person must show evidence that

[6] *Protecting Consumer Privacy in an Era of Rapid Change* FTC, Report March 2012, located at http://www.ftc.gov/os/ 2012/03/120326privacyreport.pdf.

someone is using the number fraudulently or is being disadvantaged by the misuse.[7] Thus, a person whose PII has been stolen cannot obtain a new Social Security number until the damage has already been done.

B. Defendants' Data Breaches: The Publication of Social Security Numbers

22. On or about September 1, 2013, Defendants mailed their Privacy Notification to their customers. According to the Privacy Notification, the Privacy Notification was mailed on behalf of the "JP Morgan Chase & Co. family of companies," including but not limited to Defendants.

23. The Privacy Notification was comprised of paper folded over with the address printed on the front of the Privacy Notification. In the Privacy Notification, Defendants claim to protect PII, stating, in part:[8]

What we do

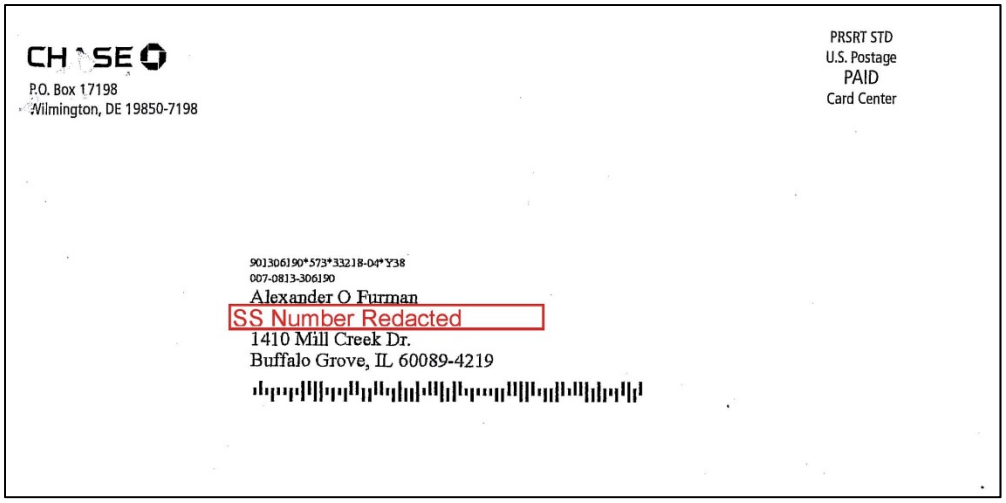
How does Chase protect my personal information?

To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. We authorize our employees to get your information only when they need it to do their work, and we require companies that work for us to protect your information.

24. However, on the front of the Privacy Notification where the mailing address was reflected, on information and belief, Defendants printed each respective customer's Social Security Number directly under their name. Plaintiff's mailing (with the Social Security Number redacted) follows:

[7] *See* Identity Theft and Your Social Security Number, SSA Publication No. 05-10064, October 2007, ICN 46327, located at http://www.ssa.gov/pubs/10064.html (last accessed September 16, 2013).

[8] https://www.chase.com/resources/consumer-privacy (last accessed September 16, 2013).


CHASE
P.O. Box 17198
Wilmington, DE 19850-7198

PRSRT STD
U.S. Postage
PAID
Card Center

901306190*573*33218-04*Y38
007-0813-306190
Alexander O Furman
SS Number Redacted
1410 Mill Creek Dr.
Buffalo Grove, IL 60089-4219

25. Upon receipt of the Privacy Notification on September 5, 2013, Plaintiff called the 1-800 number on the Privacy Notice. The representative requested that Plaintiff fax the Privacy Notification to Defendants. Because Plaintiff expressed concerns about transmitting his Social Security Number via facsimile, Defendants' representative requested that he go to his nearest Chase banking branch with the Privacy Notification.

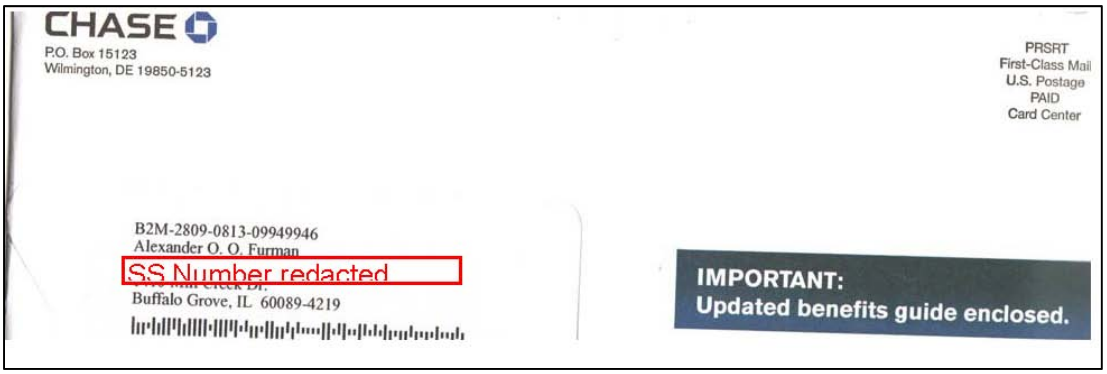
26. On the afternoon of September 5, 2013, Plaintiff went to the Arlington Heights, Illinois Chase banking branch with his Privacy Notification. The branch manager called a Security Center in San Antonio, Texas. Plaintiff, the branch manager and the Security Center representative engaged in a conference call, where the security representative apologized, told Plaintiff this never should have happened, and assured him that Defendants would rectify the situation. During this call, the Security Center representative told Plaintiff that Defendants would purchase identity theft protection on his behalf and would call him back in 10-15 minutes with a resolution.

27. Defendants never called Plaintiff back with a resolution.

28. Within 24 hours of not receiving a call back and because Plaintiff was highly concerned that his Social Security Number had been compromised, Plaintiff purchased identity theft protection for him and his son at his own expense.

29. Two days later, on September 7, 2013, Chase bank's branch manager called Plaintiff and asked if the Security Center ever called him. At that time, Plaintiff believed that the disclosure of social security numbers had happened to numerous customers, and the Security Center was focused on the overall breach, rather than on his individual case. Despite the fact that Plaintiff told the branch manager that no one had called him, Chase still has not followed up with Plaintiff nor provided a resolution for the First Data Breach.

30. On September 16, 2013, Plaintiff received another form, preprinted letter called a Benefit Notification from Defendants. Again, the outside of the mailing reflected his social security number:



31. On information and belief, Defendants printed the Social Security Numbers of the Class Members on the envelope for their updated Benefits Guide.

32. Thus, while Defendants have been on notice of the First Data Breach at least since September 5, 2013, Defendants have not taken steps to protect Plaintiff's Social Security Number nor provided a solution for rectifying the inadequate security protections that should be in place to prevent exactly this type of occurrence. As a result, the Second Data Breach occurred.

33. By printing the Social Security Numbers of Plaintiff and, on information and belief, Class Members on the front of its mailings, Defendants flagrantly disregarded and/or violated Plaintiff's and the Class Members' privacy and property rights, and harmed them in the process, by not obtaining Plaintiff's and the Class Members' prior written consent to disclose their PII to any other person—as required by the FCRA and other pertinent laws, regulations, industry standards and/or internal company standards.

34. Defendants flagrantly disregarded and/or violated Plaintiff's and the Class Members' privacy and property rights, and harmed them in the process, by failing to safeguard and protect and, in fact, wrongfully disseminating Plaintiff's and the Class Members' PII to unauthorized persons and the public domain.

35. Defendants flagrantly disregarded and/or violated Plaintiff's and the Class Members' privacy rights, and harmed them in the process, by failing to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiff's and the Class Members' PII to protect against anticipated threats to the security or integrity of such information. Defendants' unwillingness or inability to establish and maintain the proper information security procedures and controls is an abuse of discretion and confirms its intentional and willful failure to observe procedures required by law, industry standards and/or their own internal policies and procedures.

36. Defendants' wrongful actions and/or inaction directly and/or proximately caused the publication of Plaintiff's and the Class Members' PII without their knowledge, authorization and/or consent. As a direct and/or proximate result of Defendants' wrongful actions and the resulting Data Breaches, Plaintiff and the Class Members have incurred (and will continue to incur) damages in the form of, *inter alia*, (i) loss of privacy, (ii) the imminent, immediate and

continuing increased risk of identity theft and identity fraud, (iii) out-of-pocket expenses to purchase credit monitoring, internet monitoring, identity theft insurance and/or other Data Breach risk mitigation products, (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud, including the costs of placing a credit freeze and subsequently removing a credit freeze, (v) the value of their time spent mitigating the increased risk of identity theft and identity fraud, and/or (vi) deprivation of the value of their PII, for which there is a well-established national and international market.

V. CLASS ACTION ALLEGATIONS

37. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this class action as a national class action on behalf of himself and the following Class of similarly situated individuals:

> All persons who were sent any mailings, on the outside of which their Social Security Numbers were printed, from JP Morgan Chase & Co., JPMorgan Chase Bank N.A., Chase Bank USA, N.A., and/or J.P. Morgan Securities LLC.

38. The Class specifically excludes Defendants, any entity in which Defendants have a controlling interest, Defendants' officers, directors, agents and/or employees, the Court and Court personnel.

39. On information and belief, the putative Class is comprised of thousands, if not millions, of geographically dispersed people, making joinder impracticable. Disposition of this matter as a class action will provide substantial benefits and efficiencies to the parties and the Court.

40. The rights of Plaintiff and each other Class Member were violated in a virtually identical manner as a direct and/or proximate result of Defendants' willful, reckless and/or negligent actions and/or inaction and the resulting Data Breaches.

41. Questions of law and fact common to all Class Members exist and predominate over any questions affecting only individual Class Members including, *inter alia*:

a) Whether Defendants violated the Fair Credit Reporting Act by failing to properly obtain, maintain, secure or protect Plaintiff's and the Class Members' Social Security Numbers;

b) Whether Defendants violated state consumer protection acts by publishing Social Security Numbers on the outside of mailings;

c) Whether Defendants willfully, recklessly and/or negligently failed to maintain and/or execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the Class Members' Social Security Numbers;

d) Whether Defendants were negligent in failing to properly safeguard and protect Plaintiff's and the Class Members' Social Security Numbers;

e) Whether Defendants owed a duty to Plaintiff and the Class Members to exercise reasonable care in safeguarding and protecting their Social Security Numbers;

f) Whether Defendants breached their duty to exercise reasonable care in failing to safeguard and protect Plaintiff's and the Class Members' Social Security Numbers;

g) Whether, by publicly disclosing Plaintiff's and the Class Members' Social Security Numbers without authorization, Defendants invaded their privacy; and

h) Whether Plaintiff and the Class Members sustained damages as a result of Defendant's failure to safeguard and protect their Social Security Numbers.

42. Plaintiff and his counsel will fairly and adequately represent the interests of the Class Members. Plaintiff has no interests antagonistic to, or in conflict with, the Class Members' interests. Plaintiff's lawyers are highly experienced in the prosecution of consumer class action cases.

43. Plaintiff's claims are typical of the Class Members' claims in that Plaintiff's claims and the Class Members' claims all arise from Defendant's failure to properly safeguard and protect their Social Security Numbers, and by publishing the Social Security Numbers.

44. A class action is superior to all other available methods for fairly and efficiently adjudicating Plaintiff's and the Class Members' claims. Plaintiff and the Class Members have been harmed as a result of Defendant's wrongful actions and/or inaction and the resulting Data Breaches. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Defendants' conduct.

45. Class certification, therefore, is appropriate pursuant to Fed. R. Civ. P. 23(b)(3) because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

46. Class certification also is appropriate pursuant to Fed. R. Civ. P. 23(b)(2) because Defendants have acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

47. The expense and burden of litigation would substantially impair the ability of Class Members to pursue individual lawsuits in order to vindicate their rights. Absent a class action, Defendants will retain the benefits of its wrongdoing despite its serious violations of the law.

VI. CAUSES OF ACTION

COUNT I
WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT

48. Plaintiff incorporates the above allegations as if fully set forth herein.

49. The FCRA requires consumer reporting agencies to adopt and maintain procedures for meeting the needs of commerce for consumer credit, personnel, insurance and other information in a manner fair and equitable to consumers while maintaining the confidentiality, accuracy, relevancy and proper utilization of such information. 15 U.S.C. § 1681(b).

50. The FCRA defines a "consumer reporting agency" as:

> Any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

15 U.S.C. § 1681a(f).

51. The FCRA defines a "consumer report" as:

> [A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes, or any other purpose authorized under [15 U.S.C. §] 1681(b).

15 U.S.C. § 1681a(d)(1).

52. Defendants are Consumer Reporting Agencies as defined under the FCRA because on a cooperative nonprofit basis and/or for monetary fees, Defendants regularly engage, in whole or in part, in the practice of assembling Plaintiff's and the Class Members' PII for the purpose of furnishing Consumer Reports to third parties in connection with assessing eligibility for credit.

53. Plaintiff's and the Class Members' PII constitute Consumer Reports because they bear on, *inter alia*, their credit worthiness, credit standing, credit capacity, character, general

reputation, personal characteristics, physical/medical conditions, and mode of living, which is used or collected, in whole or in part, for the purpose of establishing Plaintiff's and the Class Members' eligibility for credit to be used primarily for personal, family, or household purposes.

54. As Consumer Reporting Agencies, Defendants were required to adopt and maintain procedures designed to protect and limit the dissemination of consumer credit, personal, and other information in a manner fair and equitable to consumers while maintaining the confidentiality, accuracy, relevancy, and proper utilization of such information. Defendants, however, violated the FCRA by failing to adopt and maintain such protective procedures which, in turn, directly and/or proximately resulted in the wrongful dissemination of Plaintiff's and the Class Members' Social Security Numbers into the public domain.

55. Defendants' violations of the FCRA, as set forth above, were willful or, at the very least, reckless, constituting willfulness.

56. As a direct and/or proximate result of Defendants' willful and/or reckless violations of the FCRA, as described above, Plaintiff's and the Class Members' Social Security Numbers were made accessible to unauthorized third parties in the public domain and compromised.

57. As a further direct and/or proximate result of Defendants' willful and/or reckless violations of the FCRA, as described above, Plaintiff and the Class Members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described in detail above.

58. Plaintiff and the Class Members, therefore, are entitled to compensation for their actual damages including, *inter alia*, expenses for adequate credit monitoring and identity theft insurance, out-of-pocket expenses, such as costs for placing a credit freeze or removing a credit

freeze, loss of privacy, deprivation of the value of their PII, and other economic and non-economic harm (as detailed above), or statutory damages of not less than $100, and not more than $1,000, each, as well as attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. § 1681n(a).

COUNT II

NEGLIGENT VIOLATIONS OF THE FAIR CREDIT REPORTING ACT

59. Plaintiff incorporates the above allegations as if fully set forth herein.

60. Defendants owed a duty to Plaintiff and the Class Members to safeguard and protect their Social Security Numbers. In the alternative, and as described above, Defendants negligently violated the FCRA by failing to adopt and maintain procedures designed to protect and limit the dissemination of Plaintiff's and the Class Members' Social Security Numbers for the permissible purposes outlined by the FCRA which, in turn, directly and/or proximately resulted in the theft and wrongful dissemination of Plaintiff's and the Class Members' Social Security Numbers into the public domain.

61. It was reasonably foreseeable that Defendants' failure to maintain procedures to safeguard and protect Plaintiff's and the Class Members' Social Security Numbers would result in an unauthorized third party gaining access to their Social Security Numbers for no permissible purpose under the FCRA.

62. As a direct and/or proximate result of Defendant's negligent violations of the FCRA, as described above, Plaintiff's and the Class Members' Social Security Numbers were made accessible to unauthorized third parties in the public domain and compromised.

63. As a further direct and/or proximate result of Defendants' negligent violations of the FCRA, as described above, Plaintiff and the Class Members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described in detail above.

64. Plaintiff and the Class Members, therefore, are entitled to compensation for their actual damages, including, *inter alia*, expenses for adequate credit monitoring and identity theft insurance, out-of-pocket expenses, such as costs for placing a credit freeze or removing a credit freeze, loss of privacy, deprivation of the value of their PII, and other economic and non-economic harm (as detailed above), as well as attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. §1681o(a).

COUNT III

VIOLATION OF ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT, 815 ILCS § 505/1 ET SEQ., AND SIMILAR STATE LAWS

65. Plaintiff incorporates the above allegations as if fully set forth herein.

66. The State of Illinois and many of its sister states have implemented laws designed to limit the use and dissemination of Social Security Numbers in an effort to counteract the growing threat of identity theft. An important aspect of these state laws prohibits the printing of Social Security Numbers on a postcard, outside of an envelope, or inside a mailing if visible through an envelope.

67. For example, Section 2RR of the Illinois Consumer Fraud Act, 815 ILCS §§ 505/2RR provides in pertinent part:

> Sec. 2RR. Use of Social Security numbers.
>
> (a) Except as otherwise provided in this Section, a person may not do any of the following:
>
> * * *

> (5) Print an individual's social security number on any materials that are mailed to the individual, unless State or federal law requires the social security number to be on the document to be mailed. *** A social security number that may permissibly be mailed under this Section may not be printed, in whole or in part, on a postcard or other mailer that does not require an envelope or be visible on an envelope or visible without the envelope having been opened.

68. Defendants violated Section 2RR of the Illinois Consumer Fraud Act and similar state statutes when it printed Plaintiff's Social Security Number and, on information and belief, the Social Security Numbers of the respective Class Members on the outside of the mailings in the Data Breaches.

69. Defendant's violations of state consumer fraud acts proximately caused injury to Plaintiff and members of the Class.

70. Pursuant to 815 ILCS § 505/10a and similar state laws, Plaintiff is entitled to actual damages, punitive damages, and reasonable attorneys' fees and costs, as well as any other relief the Court deems proper.

COUNT IV

NEGLIGENCE

71. Plaintiff incorporates the above allegations as if fully set forth herein.

72. Defendants owed a duty to Plaintiff and the Class Members to safeguard and protect their PII.

73. Defendants breached their duty by failing to exercise reasonable care and failing to safeguard and protect Plaintiff's and the Class Members' PII.

74. It was reasonably foreseeable that Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class Members' PII would result in the unauthorized disclosure of Plaintiffs' Social Security Numbers.

75. Plaintiff and the Class Members were (and continue to be) damaged as a direct and/or proximate result of Defendants' failure to secure and protect their PII in the form of, *inter alia*, expenses for adequate credit monitoring and identity theft insurance, out-of-pocket expenses, such as costs for placing a credit freeze or removing a credit freeze, loss of privacy, deprivation of the value of their PII, and other economic and non-economic harm (as detailed above), for which they are entitled to compensation.

76. Defendants' wrongful actions and/or inaction and the resulting Data Breaches constituted (and continue to constitute) negligence at common law.

COUNT V

INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE FACTS

77. Plaintiff incorporates the above allegations as if fully set forth herein.

78. Plaintiff's and the Class Members' PII was (and continues to be) sensitive and personal private information.

79. By virtue of Defendants' failure to safeguard and protect Plaintiff's and the Class Members' PII and the resulting Data Breaches, Defendant wrongfully published and disclosed Plaintiff's and the Class Members' PII to unauthorized persons.

80. Plaintiff's and the Class Members' PII is not of a legitimate public concern; publicity of their PII was, is and will continue to be offensive to Plaintiff and the Class Members.

81. Plaintiff and the Class Members were (and continue to be) damaged as a direct and/or proximate result of Defendant's invasion of their privacy by publicly disclosing their Social Security Numbers.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, respectfully requests that (i) this action be certified as a class action; (ii) Plaintiff be designated the Class Representative; and (iii) Plaintiff's counsel be appointed as Class Counsel. Plaintiff, on behalf of himself and the Class Members, further requests that judgment be entered against Defendants, in favor of Plaintiff and the Class Members, for:

(i) actual damages, consequential damages, statutory damages and/or nominal damages in an amount to be determined by the trier of fact;

(ii) punitive damages;

(iii) injunctive relief;

(iv) pre- and post-judgment interest at the highest applicable legal rates;

(v) attorneys' fees and litigation expenses incurred through trial and any appeals;

(vi) costs of suit; and

(vii) such other and further relief that this Court deems just and proper.

JURY DEMAND

Plaintiff, on behalf of himself and the Class Members, respectfully demands a trial by jury on all of his claims and causes of action so triable.

DATED: September 19, 2013

HAGENS BERMAN SOBOL SHAPIRO LLP

By: /s/ Elizabeth A. Fegan

Elizabeth A. Fegan
Daniel J. Kurowski
HAGENS BERMAN SOBOL SHAPIRO LLP
1144 W. Lake St., Suite 400
Oak Park, IL 60301
Telephone: (708) 628-4960
Facsimile: (708) 628-4950
E-mail: beth@hbsslaw.com
dank@hbsslaw.com

Steve W. Berman
HAGENS BERMAN SOBOL SHAPIRO LLP
1918 Eighth Ave., Suite 3300
Seattle, WA 98101
Telephone: (206) 623-7292
Facsimile: (206) 623-0594
E-mail: steve@hbsslaw.com

David Freydin
Timothy A. Scott
THE FREYDIN LAW FIRM LLP
8707 Skokie Blvd, Suite 305
Skokie, IL 60077

Attorneys for Plaintiff and the Proposed Class